Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2009 Proceedings

Americas Conference on Information Systems (AMCIS)

2009

A First Approach in the Assessment of the Complexity of Disaster Recovery Models for SMEs

Olivia F. Lee
St. Cloud State University, oflee@stcloudstate.edu

Dennis C. Guster
St. Cloud State University, scguster@stcloudstate.edu

Mark B. Schmidt
St. Cloud State University, mark@stcloudstate.edu

A First Approach in the Assessment of the Complexity of Disaster Recovery Models for SMEs

Olivia F. Lee
St. Cloud State University
oflee@stcloudstate.edu

Dennis C. Guster
St. Cloud State University
dcguster@stcloudstate.edu

Mark B. Schmidt
St. Cloud State University
mark@stcloudstate.edu

ABSTRACT

In an organization, a well devised disaster recovery plan is not only crucial in the information recovery process, but also vital in the quest to sustain daily operations. While prior research has discussed many recovery sites options, assessment of recovery site communication paths and their associated complexity is still limited in regard to the evaluation of disaster recovery (DR) models. Using the scale-free degree distribution formula, the authors present a methodical discussion concerning the network characteristics of various disaster recovery options. This study marks a pioneering effort in the DR field by applying the scale-free degree distribution formula to assess the network complexity index and overall model failure points. In addition, a modified hot model employing host virtualization designed especially for small and medium size businesses is presented. This method is particularly advantageous to small and medium size businesses as it leverages inexpensive commercial PC hardware.

Keywords
Disaster recovery, degree of distribution, recovery site options, network complexity, failure point, small and medium size business, SME

INTRODUCTION

Information systems enable SMEs to increase their effectiveness in the global environment (Montazemi, 2006). However, due to various threats facing information assets, adequate care must be taken to insure continued operations should a catastrophic event occur. Thus it is important to have a plan. The need to invoke a disaster recovery plan can occur as a result of many factors. Typically the cause of the interruption is due to a natural or man-made disaster. A disaster can occur in many forms, including flooding, power outage, fire, vandalism and theft. Organizations must take steps to protect their information assets from such things as natural disasters, power outages, and even terrorist attacks (Kenneth, Kendall, and Lee 2005). In the analysis of electronic data recovery, there are many options available to protect data and ensure business continuity. Backup system options such as external removable hard drives or similar devices are simply not effective, if that data is not protected offsite. Therefore, it is important to have a plan in place to transition control of business operations for even a brief period when a disaster strikes (Hill 2008). Further, this planning can save thousands of dollars of unnecessary expenses. In some cases, SMEs may tend to ignore security risks in favor or implementing technological solutions (Schmidt, Johnston, and Arnett, 2004).

It is increasingly important to maintain continuous access to information systems in today's global business environment (Clitherow, Brookbanks, Clayton, and Spear 2008). A disaster recovery (DR) plan ensures the continuation and progression of business regardless of single or multi-point failures by offering redundant systems and multi-point backups which are designed to provide multiple recovery options. Initiating a quick recovery is vital if the crippling effects associated with a work stoppage are to be avoided. The objective of a disaster recovery plan is to return the business to operational status as close as possible to the status before the disaster occurred (Toigo, 2002). Thus, recovery efforts must ensure any possible failure can easily be reversed and critical information can be restored to the point where business may take place as usual (Toigo, 1996). This important goal must be fulfilled to make certain repeated disasters do not cause degradation of business performance as a whole.

The planning and implementation of a successful disaster recovery strategy can be quite complex and highly customized to a firms' business nature (Krojnewski and Nager, 2006). For many small and medium size businesses, budget constraints often preclude the adoption of a sophisticated disaster recovery plans that offer promising recovery time and well organized recovery processes (Balarous, 2008). Specifically, most challenges related to DR planning are related to complexity of communication paths and failure points. While the concept of model complexity is somewhat related to system failure the true value may be in assessing the model complexity from a personnel support perspective. In the current IT environment, hardware is relatively cheap and therefore creating complex models with very high degrees of fault tolerance is easily accomplished. However, devising, configuring, maintaining and understanding how they apply to data takes a substantial commitment in terms of personnel. Because personnel is typically the greatest cost within the IT budget, understanding and applying model complexity can be a very useful tool in assessing the potential personnel costs related to any disaster recovery model. Instead of focusing on expensive options that are beyond small and medium sized business' DR budget, this paper proposes the adoption of a modified hot site that leverages standard commercially available PC hardware.

OVERVIEW OF DISASTER RECOVERY SITE OPTIONS

Since no organization is immune to the possibility of a disaster, and the danger of centralizing all data and logistics in a single location is often not heeded the resulting risk may translate to very costly consequences if the company is unable to function following a disaster. To mitigate risk, the solution lies in having devices and technologies available which allow organizations to regain access to their vital information systems within a reasonable timeframe while at a cost they can afford. It is true that DR plans can vary greatly in sophistication and cost (Yamato et al, 2006). While the simplest plan might only involve a tape backup, the most complex might feature fault tolerance on multiple levels and might be similar to the plan offered by Wang et al. (2006). It is critical that organizations devise a cost effective DR plan that can be easily deployed to ensure business continuity. A plan of this type must meet feasibility, consistency, reliability, and specific IT environment characteristics. Dealing with these important issues related to whether or not the DR plan is feasible in terms of human resources, technology infrastructure and recovery time must be addressed early in the DR planning stage (Bryson et al., 2002).

Typically DR backup strategies are organized into three data back-up site categories: cold, warm or hot sites. Figure 2 provides a graphical representation that depicts the three available options in regard to recovery expenses (investment) versus recovery time. Infrastructure complexity and investment cost are the two major issues to guide ascertaining the appropriate DR model. In the case of small and medium-sized businesses, the availability of technical resources and DR budget limitations are factors that dictate reasonable recovery spending, but can still yield effective benefits. Therefore, decisions related to allocating these resources are important to ensure that organizational sustainability is maintained. Bryson et al. (2002) states the importance of using mathematical models to analyze and design DR models. Prior model analysis indicates that the more physical components (hosts) in a DR infrastructure, the greater the probability of a hardware failure. While, additional hardware can provide a higher degree of fault tolerance that hardware will also increase the DR expense from both the hardware and personnel perspective.

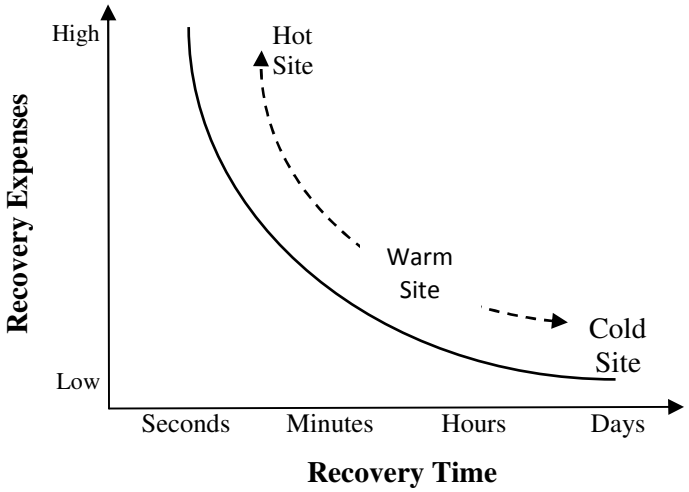

Figure 1 Recovery Expenses versus Recovery Time.

COMPARISON AMONG DISASTER RECOVERY MODELS

Building on prior use of complexity modeling, we employ the scale-free degree distribution theory to ascertain network growth by applying the formula: N*(N-1)/2 to assess the complexity of the communication paths within each DR model (Boccaletti et al., 2006). The logic is based on the premise that a complex model will result in higher possible failure points and be more difficult to support from a personnel perspective. The formula allows us to determine the complexity of communication paths and possible failure points, based on the total number of computer hosts in a production environment and the configuration of the replication process. The basis for this comparison begins with the first example (Basic Computation of Failure Points) in Table 1, which is a simple client/server model that typically consists of a client computer, a server computer and a network connecting those two computers together and would have a complexity index of one and three total model failure points.

Description		**No. of computers per instance**	**Network Complexity**	**Individual failure points per instance**	**Total model failure point**	
Formulae		N	C = N*(N-1)/2	IFP = N+C	TMFP = I*IFP	
Basic Computation of Failure Points		2	2*(2-1)/2 = 1	2+1 = 3	1*3 =3	
Cold	Based on a 6-host Example	2	2*(2-1)/2 = 1	2+1 = 3	6*3 = 18	
Warm	Production Site	6	6*(6-1)/2 = 15	6+15 = 21	1*21 =21	21+18+1 = 40
	Back-up Site	2 (per instance)	2*(2-1)/2 = 1	2+1 = 3	6*3=18	
	WAN connection				1	
Modified Hot	Production site	3	3(3-1)/2=3	3+3=6	1*6=6	6+3+1 = 10
	Back-up Site	2	2(2-1)/2=1	2+1=3	1*3=3	
	WAN connection				1	

Hot	Production site	18	18(18-1)/2=153	18+153=171	1*171= 171	171+78+2 =251
	Back-up Site	12	12(12-1)/2=66	12+66=78	1*78=78	
	WAN connection				2	

Table 1. Network Complexity and Total Model Failure Points

Note in the above example (Basic Computation of Failure Points), a network complexity of one reflects a very simple model. The individual possible failure point is three, and is arrived at by adding the number of computers (N) to the network complexity (C) indicating that there are three possible failure points. Because this backup scenario is applied to only one production host (1 instance) in the example, the total model failure points is still 3. In the remainder of the computations, we based our assumptions on a six-host production model because such a number is regarded as a representative model for most small and medium sized businesses. Furthermore, that is the number of production hosts in our computing domain and we had experience working with that number. Also note that any number of hosts (computers) might occur. However, it is common occurrence in organizations to have separate hosts for various applications such as accounting and inventory to manage security and performance indicators. From a network management perspective, additional hosts are often required to support networking activities such as World Wide Web (WWW), domain name service (DNS) and remote file systems (RFS).

Cold Site Model

The cold site is typically the least expensive back-up option to operate. It involves minimum cost to set up because there are no functioning back-up copies of the data at the primary location, or of the data center on or off site, and often little or no additional hardware is required if the tape backup systems are already available. In this model, the methodology used would be a restoration from tape to newly purchased hardware with only the daily granularity level provided by the backup. This simple form of the DR model requires additional time to recover data following any disaster and up to a day's worth of data could be lost. Based on our proposed 6 host model it would be necessary to backup six hosts (i.e., computers). Each host is backed up independently. Hence, for any one backup option, only a host and a tape backup storage device are required.

As shown in Table 1, the scale-free degree distribution formula can be applied to find out the complexity of a cold site model of a host/tape backup pair, 2*(2-1 host)/2 = 1. Therefore, the network complexity for this one instance equals one. When adding this value to the number of hosts (computers) required, the possible individual failure points becomes three, similar to the standard simple client/server example delineated earlier. However, in a 6-host model, all six computer pairs are functioning independently and thus each pair's failure points must be accounted for separately. Thus, the resulting number of network failure points is the product of total number of instances (6 hosts) and individual failure points (3).

Warm Site Model

The warm site offers a higher degree of sophistication and features an alternate location where data could be relocated after disruption. It is often equipped with hardware much like the primary site but does not store exact copies of the data. The granularity is improved as compared to the cold site and often the updates take place on an hourly basis. A warm site then can be viewed as moderately expensive to operate and the cost is a function of the recovery speed desired. It might feature the same technological capacity as the primary site, depending on the recovery time objectives (RTO) and recovery point objectives (RPO). Thus, data could often be restored onto available equipment at this site to resume business operations, but would typically take longer than at the hot site model.

Using the base assumption of a six-host production model, our warm site model would require six local and 12 remote hosts, whereby there are two remote replicas for each production host. The logic is that in the event of a disaster at the production site, one replica in each pair would become the production host which would still leave one replica for backup in each pair. The production hosts are configured to share data for backup and performance purposes. This is because in a distributed network, all data required by a given host is not going to reside entirely on a production host itself. Data are transferred across all hosts and thus it is crucial that all hosts have the ability to communicate with each other. As a result, any given replica in the replica set must offer a high degree of flexibility and fault tolerance. In essence, this is an extension of the local network area (LAN) replication method that uses the redundant array of inexpensive hosts (RAIH) logic but is expanded

across a wide area network (WAN) to provide remote replication in case the LAN site and its production hosts are compromised.

Since each site is designed to be a mirror of each other, the typical warm-site model would require the production site to have host interaction capability, and the remote site would be equipped with a series of independent connections. This structure allows great improvement in recovery granularity but is very sensitive to the timely data update process due to WAN speed dependency as well as the back-up synchronization process. The major advantage of this option is a higher degree of fault tolerance and recovery outcomes, but the recovery investment is also significantly higher than the previous cold model.

In this case as shown in Table 1, the production site has 21 IFP, while the remote site 3 IFP. Such a remote site scenario occurs six times because our model contains six hosts. Hence the remote site complexity is 18. The total complexity is 21(main site) + 18 (remote site) +1(WAN connection) = 40. Therefore, in the total model there are then 40 possible failure points.

Hot Site Model

A hot site is the most expensive option, it offers full technological capacity to enable a seemingly fool-proof recovery process. Due to the complexity of their infrastructure, hot sites provide real time synchronization between the primary and alternate back-up site, allowing a complete mirroring of the original data using wide area network links (in our case two independent leased links) and advanced software. Following a disruption to the primary location, the data processing can be relocated quickly to the hot site with minimal loss to routine operations (e.g., Yamato et al., 2006). In any commercially operated hot site, it is assumed that full connectivity to the newly assigned production hosts within each site can be achieved within a matter of a few seconds after a disaster.

While a hot site model offers the best fault tolerance and recovery times, it is the most expensive and sophisticated in terms of technology infrastructure. More than likely, it is way beyond the budget allowance of most small and medium sized businesses. In the hot model fault tolerance has been maximized and recovery granularity minimized. In many hot site options, a RAIH model (with a redundant array of inexpensive disks also employed) is used to maximize flexibility and fault tolerance. At the main site each host is replicated twice, while at the remote site it is also replicated twice. Hence, if a main host is compromised there will be twice the chance to recover either locally and remotely. This means if the entire main site is lost, the network has twice the chance to recover at its remote site. Further, the main and remote site (it is possible to have more than one remote site at added cost, but our model does not for the sake of simplicity) must be connected via a high speed wide area network (WAN) connection(s) so that the remote replicas are updated in real time. Even if the entire main site is lost, little or no data would be lost.

Based on a six- host assumption in the Table 1, the local site would have 18 computers and then 153 as its Network Path Complexity. Thus, IFP would be 171. At the remote site, we have to replicate 6 hosts two times each (there are no main hosts here they are at the main site), hence 66 Network Path Complexity, which result in 78 IFP. Therefore, the total model complexity (TMFP) after adding the 2 WAN connections is 251.

Modified Hot Site Model

A modified hot site is a recovery option that provides the partial benefits of a hot site with a less of a DR investment. The concept of applying virtualization to this type of model is described in (Guster, et al, 2008). We recognized the potential of virtualization and devised this DR option based on the success we had in leveraging the benefits of host virtualization for creating multiple logical computers (partitioning the resources of one physical computer into six virtualized resource sets) in one single physical computer. Because all production hosts are virtualized into one physical host, this option generates a smaller complexity index and as a result, it also has fewer failure points. A modified hot model is an attractive alternative to most small and medium size businesses that cannot afford to adopt a hot site option due to a limited DR budget. While the modified-hot side option will not offer recovery granularity of a true hot site, its basic performance is stable and often within acceptable boundaries. Perhaps most importantly, this option requires minimum investment and thus it is a very cost effective alternative. Instead of six physical hosts as featured in a traditional warm or hot site, only one physical host is required to be configured to house the original six hosts. Thus, all data resides on one single machine. Using a common analogy, this is similar to putting "all your eggs in one basket". However, the logic is to have multiple "baskets" to minimize risks.

In this model the one virtualized physical host (but containing 6 logical hosts) is replicated twice at the main site (each replica contains 6 virtual hosts as well). At the production site, the network complexity for this model is 3 because it has 3 physical hosts. Its IFP would be 6. The remote site would require only 2 replications of the main production host at the main site. Which would be calculated as follows 2 (physical hosts)*(2-1)/2 = 1(network path complexity), plus the 2 hosts = 3 (remote site complexity). There is one internet WAN connection Therefore, the total model complexity is 10 (6 + 3 + 1 = 10).

DISCUSSION

In the prior section, four disaster recovery options were compared and an assessment of network complexity and failure points was carried out. The selection process of recovery site options relies on the infrastructure required and its associated investment including maintenance cost. Fundamentally, the infrastructure requirements consist of hardware, software and personnel costs. Within each model the replication process contains at least daily backups and is synchronized across replicas in case of a single geographically localized emergency such as a fire or flood (in the cold site model hopefully the tapes would at least be stored off site). All these plans require keeping a mirror image of the data for later use in the recovery process. Sophisticated plans as presented by Abhang and Chowdry (2007) allow multiple image back-ups and quick recovery time. However, these models require expensive and highly advance equipment such as SANs (storage area networks) or other complex storage devices. Generally speaking, higher complexity may result in higher reliability, but will also incur higher technology infrastructure and associated personnel cost. Instead of focusing on expensive options, we propose the use of a modified hot site as a practical solution that relies on inexpensive commercial hardware components (Table 2 and Table 3).

Model	Synchronize Time	Recovery Time	Back-up Site Characteristics	No. of Hosts	Tolerance Support
Cold	Days	>24 Hours	Off site backups	12	Limited
Warm	Hours	1-24 hours	Limited physical mirroring	18	Moderate
Modified Hot	Minutes	1 hour	Virtual mirror image	6	High
Hot	Seconds	Minutes	Physical mirror image	30	Very high

*Based on a 6-host model

Table 2: Disaster Recovery Models*

Recovery Sites	Software: Server Site [1)]	Hardware: Remote Site [2)]	Bandwidth Cost (WAN) [3)]	Personnel Cost [4)]	Total Cost:
Cold	2,500	6,000	0	10,400	18,900
Warm	5,000	6,000	4,800	26,000	41,800
Modified Hot	0	3,000	1,200	13,000	17,200
Hot	50,000	120,000	120,000	52,000	342,000

*Based on a 6-host model

Table 3: Disaster Recovery Investment and Annual Maintenance Costs

1) *Software Costs*: a commercial tape backup package with 6 licenses for the cold, a commercial backup/replica package with 6 licenses for the warm, use of shareware software at no cost for the modified hot and an enterprise level backup replica package with an unlimited server license for the hot.
2) *Hardware Costs*: 6 low end PCs with tape drives @ $1,000 each (this allows for simultaneous backup of all six hosts) for the cold, six mid range server level hosts @$1,000 each for the warm, three mid range server level hosts @$1,000 each for the modified hot, 12 high range enterprise server level hosts @$10,000 each for the hot site.
3) *Bandwidth Costs*: the tape backup equipment would reside on site so there are no WAN bandwidth requirements for the cold, leased line (point to point) at 300 miles at 12mbs for the warm, internet cable connection at 10mbs (VPN configured for security) for the modified hot and dual 40 mbs leased lines at 300 miles for the hot.
4) *Personnel Cost*: tape operations personnel @10 hours a week at $20 an hour for the cold, 10 hours a week at $50 an hour for system/network engineering personnel for the warm, 5 hours a week (due to reduced hardware) at $50 an hour for system/network engineering personnel for the modified hot and 20 hours a week (due to added hardware) at $50 an hour for system/network engineering personnel for the hot site.

The network infrastructure in selecting a recovery site option is also important criteria. The network infrastructure involves line speed, topology, and type of connections such as WAN or LAN. It is important to note that any change made to the production host must propagate to all other replicas of that host or file system. For remote replicas, the update process also requires a WAN connection. The algorithm used in this replication process can have an impact on the complexity of the network infrastructure. Complexity may be beneficial if it increases the degree of fault tolerance. However, if adequate WAN bandwidth is not provided then the desired granularity will not be obtained. Conversely, a high performance bandwidth investment may not be worthwhile or cost effective when inadequate model design causes the updating process to be inherently slow and once again in this situation the desired recovery granularity becomes unattainable (Kunet al., 2006). Therefore, instead of solely relying on replication in a WAN environment, small and businesses should consider replication in a local area network (LAN) as the first line of defense. LANs provide speedy and inexpensive network configurations and can support reasonably sophisticated replication methods. Ultimately however, data will need to be replicated remotely. To improve efficiency, remote replica models must incorporate data stream optimization and better tuning than LAN models. Therefore, compression strategies and only updating the data that actually changes instead of a complete replica copy are paramount in getting the most out of a speed limited WAN link.

CONCLUSION

Since the inception of IT, the need to develop an effective DR plan is well documented in both academic and practitioner literature. To understand one of the key issues in selecting a recovery site, it is helpful to assess the complexity of a chosen model's communication path and its possible failure points. Actually, the most challenging decisions surrounding DR planning are related to selecting the appropriate number of hosts, degree of fault tolerance desired, the appropriate granularity and then attaining all of those goals within the available budget. Disaster tolerance as previously stated is the ability to maintain ongoing productive operations even if a catastrophe occurs. This is an important outcome since high availability is achieved by providing redundant components; if one fails, another part is still available to do the job. Applying the scale-free degree distribution formula, this paper demonstrates how a complexity index of various recovery models can be computed and how to identify potential network failure points. The paper also proposes the adoption of a modified hot site for its cost effectiveness and benefits that are very similar to those of the hot site option.

One study shows that only 37% of health maintenance organizations (HMOs) have adequate DR plans (Bandyopadhyay, 2001). This is discouraging given the important and sensitive nature of the information maintained by an HMO. There appears to be a dearth of research focused on assessing the number of SMEs that have DR plans. However, given the increasing importance of information systems in organizations, it is assumed that the percentage of SMEs with adequate DR plans is less than it should be. As previously stated, the key advantage of the proposed modified hot site is cost effectiveness. By deploying virtualization to reduce the number of physical hosts and using shareware software, firms can develop a structured and actionable DR plan that attains many of the benefits of a hot site model. The cost effective nature of this model may assist SMEs to develop adequate DR plans. The application of virtualization is a formal approach to DR planning which enables effective DR solutions that are less complex, cost effective and close to the performance level of the hot model. As we suspected there was a relationship between the complexity coefficient we generated and cost. The virtual model reduced the level of complexity by a factor of about 20 while at the same time maintaining adequate coverage at a reasonable cost. We would suspect that there may be a need for hybrid models that use both the traditional physical host model and virtualization that may be adaptable for hot site functions. In designing and assessing those model we feel our complexity checking methodology may be quite useful in the objective decision making process. From a practical perspective we feel that our virtual option in its present form is a very attractive solution for small and medium sized businesses due to its simple design which enables firms to easily map out the dependencies between critical business processes, people, IT assets, and budget constraints. It can also perform simultaneous functions in hosting DNS, maintaining a global file system, enabling website service, allowing email communication, serving as a firewall, and providing instructional support all in a single physical host, while still maintaining the separation of those services for performance and security purposes.

REFERENCES

1. Abhang, S. and G. Chowdry (2007). WDM-Based Storage Area Networks for Disaster Recovery Operations, International Journal of Computer, Information, and System Science and Engineering, 1(4).
2. Balaouras, Stephanie (2008), "Building the Business Case For Disaster Recovery Spending," *Forrester Report*, April 3, 2008.
3. Bandyopadhyay, K. (2001). "The Role of Business Impact Analysis and Testing in ***Disaster Recovery*** Planning by Health Maintenance Organizations." Hospital Topics, 79 (1).

4. Boccaletti, S., V. Latora, Y. Morento, M.Chavez and D.U. Hwang (2006), "Complex Networks: Structure and Dynamics," *Physics Reports*, 424, 175-308.
5. Bryson. Kweku-Muata (noel), Harvey Millar, Anito Joseph and Ayodele Mobolurin (2002), "Using Formal MS/OR Modeling to Support Disaster Recovery Planning", *European Journal of Operational Research*, 141, 679-688.
6. Clitherow, D., Brookbanks, M., Clayton, N. and Spear, C. (2008). *"Combining high availability and* ***disaster recovery*** *solutions for critical IT environments."*. IBM Systems Journal, 47 (4) 563-575.
7. Guster, Dennis C., Brandon P. McCann, Kira Kizenski and Olivia F. Lee (2008), "Cost Effective, Safe and Simple Method to Provide Disaster Recovery for Small and Medium Sized Businesses," *Review* of *Business Research*, 8(4), 63-71.
8. Hill, Jeffrey (2008), "Business Continuity: Implementing Disaster Recovery Strategies and Technologies", Aberdeen *Benchmark Report*, March, 2008.
9. Kendall, Kenneth E.; Kendall, Julie E.; and Lee, Kin C. (2005) "Understanding Disaster Recovery Planning through a Theatre Metaphor: Rehearsing for a Show that Might Never Open," *The Communications of the Association for Information Systems*: Vol. 16, Article 51.
10. Krojnewski, Rüdiger and Bill Nager (2006), "Disaster Recovery: It's Not Just an IT Problem," *Forrester Report*, November 13, 2006.Montazemi, Ali Reza, (2006). "How They Manage IT: ***SMES*** IN CANADA AND THE U.S." *Communications of the ACM*, 49 (12) 109-112.
11. Schmidt, Mark B; Allen C. Johnston; and Kirk P. Arnett (2004). "Wireless Network Security in Hospitality SMEs," Proceedings of the 2004 Americas Conference on Information Systems (AMCIS). August 2004, New York, NY.
12. Wang, K., Rui-dan, S., Zeng-xin, L., Zhen, C. & Z. Li-hua, (2006). "Robust Disaster Recovery System Model". Wuhan University Journal of Natural Sciences. 11(1).
13. Toigo, J.W. (1996). *Disaster Recovery Planning: For Computers and Communication Resources*. John Wiley & Sons, Inc.
14. Toigo, J.W. (2002). *Disaster Recovery Planning: Preparing for the Unthinkable*, 3rd Edition. Prentice Hall.
15. Wang, K., Rui-dan, S., Zeng-xin, L., Zhen, C. & Z. Li-hua, (2006). "Robust Disaster Recovery System Model". Wuhan University Journal of Natural Sciences. 11(1).
16. Yamato, J., Kan, M., Kikachi, Y., Takaya, M., Tomi, M. & T. Adachi (2006). "Outline of Disaster Recover Architectures", NEC Technical Journal, 1(4).